

**REMARKS**

In response to the final Official Action of February 12, 2007, claims 1, 9, 18 and 25 have been amended in a manner which is believed to distinguish the present invention over the cited art.

**Claim Rejections - 35 USC §103**

Claims 1, 3, 4, 6, 8, 9, 11, 12, 14, 16, 18, 20, 21 and 23-25 are rejected under 35 USC §103(a) as unpatentable over US patent application publication 2002/0147920, Mauro, further in view of US patent application publication 2002/0150243, Craft, et al (hereinafter Craft).

Specifically, the Office states in the section entitled "Response to Arguments" (page 22) that "The language of claim 1 does not mention that the communication between the secure processing point and the personal device have to be separated". Therefore, the Office concludes that Mauro does disclose the retrieving in a secure processing point arranged in communication with the personal device, a unique chip identifier from the personal device. Claim 1 as amended particularly points out that the secure processing point is separated from and arranged in communication with the personal device. This is clearly supported in the application as originally filed, including Figures 1 and 2 and the accompanying description, including page 8, lines 9-30.

Thus, it is respectfully submitted that Mauro does not meet the requirements of claim 1 since Mauro teaches that the secure unit (240) itself performs all secure processing and stores all "sensitive" data, which data includes any data desired to be prevented from unauthorized access (see paragraph 34). Figure 3 of Mauro is a diagram of a specific embodiment of the secure unit (240) (see paragraphs 35-40). Thus, claim 1, as amended, is specifically directed to a method for managing

cryptographic keys that are specific to a personal device and comprises retrieving in a secure processing point which is separated from and in communication with the personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device.

As seen in Figure 3 of Mauro, the secure unit (240) is within a remote terminal. This is specifically pointed out at paragraph 18 of Mauro which describes Figure 3 as a diagram of a specific embodiment of a secure unit within the remote terminal. Consequently, the retrieving in a secure processing point separated from and arranged in communication with the personal device, a unique chip identifier from the personal device is not possible in Mauro since the secure unit is part of the personal device.

Furthermore, in the Response to Arguments section (page 25), it is stated that Craft teaches receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the chip, as well as associating the unique chip identifier with the received backup data package and storing the backup data package and the associated unique chip identifier in a permanent public database. The Office asserts that the client serial number (216) in Craft is equivalent to a unique chip identifier and that a client public key datastore (222) is equivalent to a permanent public database. Even assuming such equivalency for purposes of argument, Craft does not show receiving at the secure processing point (presumably the secure datastore (226)) in response to storing the data package in the personal device (presumably the client side in Craft) a backup data package from the personal device.

Rather, Craft is directed to a method and system for controlled distribution of application code and content data within a computer network. It is shown that a client device is configured to download application code and/or content data from a server operated by a service provider. Embedded within the client is a client private key, a

client serial number and a copy of a server public key. The client forms a request which includes the client serial number, encrypts the request with the server public key and sends the download request to the server. The server in turn decrypts the request with the server's private key and authenticates the client. The received client serial number is used to search for a client public key that corresponds to the embedded client private key and thus the client public key datastore (222) cited by the Office as equivalent to the permanent public database in claim 1 is not for purposes of storing a backup data package but rather is simply a place for storing client public keys and matching those keys to serial numbers from client requests. The application code and/or contact data is then encrypted by the server so that only the requesting client can decrypt the application code and/or content data.

In short, Craft fails to disclose or suggest receiving a backup data package from a personal device, which backup data package is the data package encrypted with a unique secret chip key and is related to the data package stored in the personal device by the secure processing point. Whatever application code and/or content data that is downloaded to the client from the server in Craft is not then backed-up to the server and encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the chip from the client.

For all of the foregoing reasons, it is therefore respectfully submitted that claim 1 as amended is distinguished over Mauro in view of Craft.

Independent claims 9, 18 and 25 have been amended in a manner similar to claim 1 and therefore these claims are also believed to be distinguished over Mauro in view of Craft.

Since each of the independent claims is believed to be distinguished over the cited art, it is respectfully submitted that all of the dependent claims are further distinguished over the cited art due to their respective dependency from a claim which is believed to be allowable.

It is therefore respectfully submitted that the present application as amended is in condition for allowance and such action is earnestly solicited.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Alfred A. Fressola', is written over a horizontal line.

Alfred A. Fressola  
Attorney for Applicant  
Registration No. 27,550

Dated: May 14, 2007

WARE, FRESSOLA, VAN DER SLUYS  
& ADOLPHSON LLP  
Bradford Green, Building Five  
755 Main Street, P.O. Box 224  
Monroe, CT 06468  
Telephone: (203) 261-1234  
Facsimile: (203) 261-5676  
USPTO Customer No. 004955